DWIGHT C. HOLTON, OSB #09054
United States Attorney
District of Oregon
KEVIN DANIELSON, OSB #06586
Assistant United States Attorney
kevin.c.danielson@usdoj.gov
1000 SW Third Avenue, Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
FAX: (503) 727-1117
Attorneys for Defendant

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

STEPHEN RAHER,

Plaintiff,

v.

FEDERAL BUREAU OF PRISONS.

Defendant.

09-CV-526-ST

DECLARATION OF MICHAEL PRATER

KENT S. ROBINSON, OSB #09625
Acting United States Attorney
District of Oregon
KEVIN DANIELSON, OSB #06586
Assistant United States Attorney
kevin.c.danielson@usdoj.gov
1000 SW Third Avenue, Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
FAX: (503) 727-1117
Attorneys for Defendant

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

STEPHEN RAHER, **CV 09-526-ST**

Plaintiff, **DECLARATION OF MICHAEL PRATER**

v.

FEDERAL BUREAU OF PRISONS.

Defendant.

I, Michael Prater, declare and state as follows:

1. I am employed by Federal Bureau of Prisons (BOP). My current position is Computer Services Administrator for the North Central Regional Office. I have served in my current position since June, 2005. I have been employed by the BOP since September, 1992. My office is physically located in Kansas City, Kansas.

2. My major responsibilities as the Regional Computer Services Administrator for the North Central Region, are to ensure secure, productive, and effective management and use of all computer resources within the region. I administer a region-wide program of computer services including ADP (automated data processing) security, hardware, software, local/wide area network management and support. Additionally, I conduct staff assist visits to monitor and support the effectiveness of computer services programs and also participate in the analysis and development of national policy.

3. I have reviewed the material pertaining to the "Information Systems Equipment" section regarding computer networking requirements withheld in the contracts issued for solicitation of CAR 1, CAR 2, CAR 5 and CAR 6.

4. I am familiar with BOP practice and procedures utilized to safe guard our network structures and to ensure unauthorized access to our network, which includes all Department of Justice, Justice Unified Telecommunications Network (JUTNet). The material withheld pertaining to computer structures and their components regarding information systems equipment required by privatized facilities was removed to ensure the safety of our structural network is maintained.

5. Based upon the BOP network set-up for information systems, we identify each component that is required in order to connect to our network. By providing this listing of all components and their structure, a hacker or "sniffer", can determine where the internal

components wiring requirements are located or whether any JUTNet security flaws might be vulnerable. A "sniffer" is software that monitors and captures data across a computer network that is used by hackers to capture user id names and passwords. The need to secure the network systems information is similar to the need to secure the key cuts on your house key. Although all houses normally have locks that are opened by keys, each key may have different key cuts to limit access. This is the same for computer network systems. The infrastructure equipment identified in the withheld material, if released, would provide critical information necessary to obtaining an "electronic" key cut. This key cut or key structure would aid the "sniffer" by allowing it the ability to access our network easier and to navigate through the electronic traffic to obtain unauthorized access. The information withheld is basic "sniffer" type material which would enable someone a start to unauthorized access to our infrastructure. Although the information in the material is somewhat out dated, the structure remains the same. Information such as our infrastructure and structure of physical wiring specifications, if disclosure, could threaten our cybersecurity for all of JUTNet. Review of this material also reveals recommendations for equipment that the contractor should install to facilitate access by BOP staff to assist with any network problem resolution. If a "sniffer" where to get access to our network coupled with the information located in the withheld material, it would give the sniffer all he/she needs to break into our Department of Justice JUTNet.

6. Information security has evolved over the years. Back when this contract was drafted, information technology specialists didn't foresee at that time, that information

regarding our equipment and requirements could be used to hack or "sniff" out access to our computer systems. What we have learned over the past few years, is that technical information such as listed, if released, would provide assistance to these hackers and sniffers to gain unauthorized access. An inmate could do more damage with electronic access to our network than if he were given a key to unlock the doors. If someone were to gain unauthorized access to our electronic network databases, he or those in the public, could alter his release date by changing jail time credit information, access information on his separatees, access sensitive information on staff, etc. We have had to release portions of our SENTRY database manual which gives instructions on how to make changes in this database. This database contains sentence computations, management variables, security and custody levels, etc. Courts have ruled that because we don't give inmates access to computers there is no harm in release of portions of the instructions or the "how to" guidance for making changes in the database. If we no longer have this shield of protection on the "how to" information, we must be able to ensure we keep our shield of protection that would not allow a sniffer to break into the network. Our physical structure for computer technology components need to be afforded protection in order to ensure inmates or the public are not able to access our network.

7. By providing the exact requirements of the network infrastructure, this would provide easier access to facilitate wiretaps by "sniffers" into our network.

8. I declare under penalty of perjury that the foregoing is true and correct. 28 U.S.C. § 1746.

EXECUTED on this 28th day of October, 2010.

MICHAEL PRATER

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on November 5, 2010, I made service of foregoing: **SECOND SUPPLEMENTAL DECLARATION OF MICHAEL PRATER**, by placing a copy in a first-class postage paid envelope in Portland, Oregon, for delivery via U.S. mail to the addresses set forth below:

Stephen Raher
P.O. Box 15189
Portland, OR 97293-5189
Phone: 503-235-8446

Pro Se

/s/ Deanne Bateson
DEANNE Bateson
Legal Assistant
US Attorney's Office
(503) 727-1072